PATENT SPECIFICATION (11) 1 546 053

1 546 053

(21) Application No. 2691/78 (22) Filed 23 Jan. 1978 (19)

(31) Convention Application No. 824/77 (32) Filed 24 Jan. 1977 in

(33) Switzerland (CH)

(44) Complete Specification Published 16 May 1979

(51) INT. CL.[2] G07F 7/10

(52) Index at Acceptance
G4H 13D 14A 14B 1A TG

(54) PROCESS AND APPARATUS FOR CODING AND TESTING AN IDENTIFICATION CARD

(71) We, GRETAG AKTIENGESELLSCHAFT, a company organised under the laws of the Confederation of Switzerland, of Althardstrasse 70, 8105 Regensdorf, Switzerland, do hereby declare the invention for which we pray that a patent may be granted to us, and the method by which it is to be performed, to be particularly described in and by the following statement:-

This invention relates to an identification process, using an identification card which bears two sets of machine-readable information and on which one set of information is stored in permanent form while the other set is stored in variable form.

Identification cards are used for the machine identification of individuals, they are used as credit cards, identity cards, or for cash withdrawls from automatic cash dispensing machines and the like. The authenticity of the identification card is usually tested in a test station during a test operation.

A good identification card must have high security against forgery, i.e. security against copying by unqualified persons, e.g. to prevent unauthorised persons from entering restricted areas or to prevent cash from being withdrawn by unauthorised inidividuals.

In the known systems, security against forgery is frequently achieved by making the identification cards difficult to produce, and then only with expensive apparatus, which is economic only if the cards are mass-produced and copies of individual cards are much too expensive. The information stored on the identification cards used with these systems is usually fixed. This has the following two disadvantages. Firstly, an organization using the identification system must obtain the cards in the finally coded form from the manufacturer and cannot re-code them themselves. This has an adverse effect on the secrecy of the system. Secondly, it is not possible to store on the identification cards variable data such as the account balance of a cash account or the time balance in the case of flexible time systems.

In another known system, the card information is contained in a magnetic track in readily recordable, readable and erasable form. It is easy for the user organization to carry out re-coding, but the security against forgery of the individual card is very low. It is increased by the card-holder introducing into the test station keyboard an individual secret identification number in addition to the card information so that a check can be made for agreement with the card information.

The disadvantages here are that, firstly, the system is forgery-proof only if the secret identification number is not disclosed and, secondly, this identification number must be introduced into the keyboard for each identification operation.

In another known process for achieving good security against the forgery of identification cards, for example as described in Swiss Patent Specification No. 554 574, the readily variable main information is stored on a conventional recordable and erasable information track on the identification card, for example a magnetic track, and the permanent and individual identification information which is difficult to forge is stored differently in another part of the card which is difficult to copy. This identification information is additionally stored in the magnetic track and during the test operation it is checked to see whether it agrees with the information that is difficult to forge. Although additional storage of the individual identification information can be effected in a different coding from that used for the information that is difficult to forge, or can be incorporated in the main information, there is a permanent and detectable agreement between the information stored on the information track and the information stored in

the other form of storage, and proof against forgery is ensured only to a limited degree.

The object of this invention is to obviate all these disadvantages. Identification cards are used with the two types of storage, firstly magnetic track with readily variable information, and secondly forgery-proof type storage which is difficult to copy for permanent major information.

The forgery-proof information or selected parts thereof influence the readily variable information by means of crypto-technical methods so that it is not possible to detect any agreement between the two sets of information and the readily variable information is, in effect, just as forgery-proof as the information which is difficult to copy.

As a result of crypto-technical selection of small parts of the forgery-proof information, security against forgery is just as great as if all the forgery-proof information were used.

The process according to the invention is characterised in that the variable information, hereinafter referred to as identification information, is formed, when the card is made, by ciphering from at least selected parts of the permanent information on the card and a secret key information, and is stored on the card, and when the card is tested a test information is formed from the same selected parts of the permanent information and the secret key information and is tested for agreement with the identification information stored on the card.

In a very effective variant of the process, the type of ciphering is changed on each new test operation so that no agreement can be detected between the two types of information stored in different ways on the identification card.

The invention will be explained in detail hereinafter with reference to the exemplified embodiments illustrated in the drawings wherein:–

Figures 1a and 1b are diagrams showing the principle of an identification card in perspective (1a) and in plan view (1b);

Figure 2 diagrammatically illustrates a system for performing the process;

Figure 3 is an enlarged detail of Figure 2;

Figure 4 is a section on the line IV–IV in Figure 3;

Figure 5 is the bottom half of Figure 4;

Figure 6 is a detail of Figure 4 with a scanning device;

Figures 7 and 8 show another exemplified embodiment in elevation and in plan view; and

Figure 9 shows a detailed exemplified embodiment for performing the process.

In Figures 1a and 1b, magnetic track 2 is applied to an identification card 1, which in this case is shown as a CREDIT CARD, the track being scanned, recorded upon and erased by means of a magnetic head 3. The card also has a zone RF having a number of storage points RZ containing forgery-proof information IU. This latter information can be read by means of a scanning head 67.

The block schematic in Figure 2 diagrammatically illustrates a system for performing the method according to the invention, the storage points RZ being disposed in lines and columns of an X-Y coordinate system. By way of example, there are provided ten lines Y_1 to Y_{10} and twenty columns X_1 to X_{20} of storage points RZ, giving a total of 200 such points. Each storage point can contain 10^6 bits, so that the entire forgery-proof information on the card according to this exemplified embodiment would be $2 . 10^8$ bits. The storage points RZ may be constructed as shown in Figures 3 to 5. The scanning head 67 for scanning the storage points RZ may be controlled by control information IS via line 50 so that the information of each individual storage point can be scanned.

For line selection the scanning head is movable in the Y-direction by a stepping motor, while column selection is made through a time window as the card passes in the X-direction through a test station. Both line and column selection are conftrolled by the control information IS.

All the information flows are shown by arrows in Figure 2. The input infomration at a crypto-computer 16 provided in a test station 52 is at least the code key information IE_1 taken from a code key store 17 and at least some of the forgery-proof information IU, in the form of input information IE_2.

This input information is used for computing the output information IA_1 which is stored in the form of magnetic information IM on the magnetic track 2 by means of the magnetic head 3 either directly or indirectly via a mixer and comparator circuit 18. The coding makes it practically impossible to draw any conclusions as to the forgery-proof information IU from the magnetically stored information IM.

Such conclusions are completely impossible if additional input information IE_3 is fed to the crypto-computer 16 in the form of variable information IV generated in a generator 26. The variable information changes on each test operation, so that the output information IA_1 computed in the crypto-computer 16 and hence the magnetically stored information IM are different after each test operation. Firstly the variable information IV is introduced into the crypto-computer in the form of information IE_3 during a recording stage of the test operation, such information IE_3 participating in determining the output information IA_1 which is recorded on the magnetic track. Secondly, the variable information IV is recorded directly on the magnetic track via a

line 51 and another line 8. On the next test operation, it is then read out by means of the magnetic head 3 during the reading and test phase, and used as input information IE_3 for the crypto-computer 16 to form the output information IA_1.

These operations are described in detail hereinafter with reference to Figure 9.

The variable information IV may be a consecutive serial number which is generated in the generator 26 and assumes a new value on each test operation. The variable information IV may alternatively be date-time information taken from an electronic clock in generator 26. The variable information IV may be a random number which is taken from a noise or random generator or a pseudo-random generator in generator 26.

Each individual identification card may contain forgery-proof information differing from all the others. This provides a very high degree of security since in such a case a forger would have to undertake the very considerable task of copying each individual identification card of an organization.

Where the security requirements are not so strict, however, the forgery-proof information may be the same for all the identification cards, except for the card number, and this reduces the card production costs to some extent. Security is guaranteed by the pseudo-random selection of certain parts of the forgery-proof information by means of crypto-computers.

Some of the forgery-proof information IU may be recognition information ID_U, i.e. for example, a coded card number which differs from card to card. This information can be examined in a control station 32 in the test station 52.

This recognition information could, for example, consist of the information of some of the 200 storage points RZ containing 10^6 bits, e.g. storage point at intersection X_7, Y_3 in Figure 2.

To increase the forgery-proof characteristics, information selected from storage zone RF by means of scanning head 67 could be used as additional recognition information to the permanent information ID_U, in which case the control information IS for this selection would be output information IA_2 of the crypto-computer 16 obtained together with the permanent identification information ID_U in the form of input information IE_2 to the crypto-computer 16.

A forger would, therefore, have to copy not only a single storage point RZ but the entire card, since he does not know what storage point will be selected by the crypto-computer.

Far more forgery-proof information can be applied to the identification card 1, i.e. 2.10^8 bits, for example, than can be processed within a reasonable time. Nevertheless, the full security offered by the large and complete quantity of information can be utilised. For example, using the variable information IV in the form of input information IE_3 to the crypto-computer 16, naturally in conjunction with the code key information IE_1, it is possible to compute output information IA_2 which, by controlling the scanning head, selects from one of the 200 storage points RZ some of the forgery-proof information IU and makes it available as new input information IE_2 to the crypto-computer for computing the output information IA_1. This partial information may, for example, be just the contents of a single storage point RZ selected in pseudo-random manner in this way, i.e. in this case approximately 0.5% of the total forgery-proof information.

It is only necessary to scan and process the information of a single storage point RZ, and yet the security against forgery is as high as if all 200 storage points were taken into account, because the forger naturally does not know which storage point is selected in "random" fashion by the crypto-computer.

Figure 3 is an enlarged detail of the identification card 1 having just two reflex zones RZ shown only partially. These reflex zones RZ consist of a number of boundary surfaces R_n which extend over the width B of the zones and are separated from one another by boundary edges K. Separating zones TZ are provided between the individual reflex zones RZ. The size of a boundary surface R_n in the direction of arrow L may be 0.2 mm while the width B transversely thereof may be about 2 mm so that the reflex zone having 10 boundary surfaces forms a square measuring 2 × 2 mm^2.

The section through the identification card in Figure 4 shows that the card consists substantially of a top layer 1*b* made from a plastic and a bottom layer 1*a* made from a similar material. The bottom layer bears the boundary surfaces R with corresponding boundary edges K which form the reflex zones RZ and are separated from one another by separating zones TZ. The underside of the bottom layer 1*a* bears a magnetic track coating 2. The two card layers are rigidly connected. The top layer 1*b* of the card must therefore either be a negative of the bottom layer 1*a* or must be applied in plastic or liquid condition to the bottom layer 1*a* without, however, changing the boundary surfaces R. The connection may, for example, be made by thermal ultrasonic welding at the separating zones TZ or by gluing the entire card surface. The connection of the two layers of the card must in any case be such that subsequent separation cannot be carried out either mechanically or with solvents without damaging the bound-

ary surfaces.

Figure 5 is a section on the line V–V through the bottom card layer $1a$ (the top layer 1b has been omitted from the figure for the sake of clarity) and, as already stated, the bottom layer is divided up into reflex zones RZ and separating zones TZ. The reflex zones in turn have a number of boundary surfaces R_1–R_1 which are at different angles 2, 4, 5 and n-1 to the card plane. The arrangement of boundary surfaces R usually differs from one reflex zone to the next. In the exemplified embodiment illustrated, ten boundary surfaces each having four possible angle positions are provided per reflex zone, and this means that $4^{10} = 10^6$ reflex zones differing from one another are possible. Of course the number of boundary surfaces per reflex zone and the number of different boundary surfaces per reflex zone and the number of different boundary surfaces may differ from this exemplified embodiment. The reflex zones RZ with the basal surfaces R may each be made by means of a press die by pressing into the plastic in the plastic state or in a plastic injection process. In the exemplified embodiment, the top side of the bottom layer of the card is metallized, e.g. by vapour coating or electroplating, so that the boundary surfaces R are provided with a metal layer $1c$ which reflects light. The metal layer is removed in the area of the separating zones TZ so that a plastic layer $1d$ is available in these zones and hence ensures a good connection between the two cards.

Figure 6 diagrammatically illustrates one exemplified embodiment of an optical scanning system for the identification card. The optical scanning system together with the recording and reading head 3 for scanning the magnetic track are installed in the test station through which the identification card 1 passes in the direction of the arrow L for test purposes. A light source 5, e.g. a laser generator, delivers a fine beam of light $5a$ which falls on to the identification card and is reflected by the boundary surfaces R_1 to R_{10}. These boundary surfaces may, for example, have four different angular positions (Figure 5) so that the reflected beam of light $5b$ may be at any one of four different angles φ_1 to φ_4 in relation to the incident beam, photodiodes $P_1 - P_4$ being provided to receive the reflected beams. In the position of the card shown in Figure 6, the beam of light $5a$ meets the reflecting boundary surface R_4 and is projected in the form of a reflected beam $5b$ on to the photo-diode P_3 which delivers a photo-current to the distributor circuit 7. As the reflex zone RZ in Figure 6 passes beneath the scanning beam $5a$, ten photo-current signals are delivered in sequence by the four photo-diodes $P_1 - P_4$ according to the angular positions of the boundary surfaces R_1 to R_{10}, to the distributor circuit 7 where they are amplified and are fed, for example, after binary coding each with a different 3-bit number per photo-diode, to the output 10 of circuit 7.

Counting for the ten photo-current signals is started when the scanning beam $5a$ passes from the separating zone TZ, where there is no photo-current flowing, to the first boundary surface. The edges of the separating zones give a diffuse reflection.

The four photo-diodes P_1 to P_4 together with the light source 5 form the photo-scanning system 6 which can also traverse transversely of the direction of movement of the card to enable all the surface reflex zones to be scanned as described above. The photo-scanning system 6 together with the distributor circuit 7 forms the scanning head 67 which scans the storage points RZ containing the forgery-proof information IU.

Despite all the forgery-proof methods described above, there is still a possibility of fraud in respect of a qualified card holder having a genuine individual identification card and using his individuak memorized identification number, in cases where the identification card is used for drawing cash by means of off-line cash dispensers in which the current account position is retained on the identification card in encoded form.

To do this, before he draws the cash the authorised card holder need only copy on to magnetic tape the magnetically stored information which includes the current account position, and then draw cash from one of the dispensing machines in which the new reduced account position is simultaneously recorded in encoded form in the magnetic track. He can then over-record on this information the magnetic tape copy corresponding to the higher account position, and then draw cash from a second dispensing machine and so on.

Of course this could be prevented if cash drawings were restricted to a specific machine, in which case the number of this machine would serve as further input information for the crypto-computer. Alternatively, a minimum time limit could be introduced between two cash drawing operations, by means of the electronic clock delivering the date-time information as a variable, and this minimum time limit would be operative until the account position has been communicated to all the off-line cash dispensers.

All this is very complicated however, and it is therefore proposed that at least one of the reflex zones should be irreversibly erased after each individual card test to ensure fraud-proof inspection via the number of card tests.

As shown in Figures 7 and 8, this can be

effected by the card material containing a thermaloy blackenable substance used in thermographic printing. Triggered by an input 13, a pin 11*a* is heated in an erase head 11 of a heater coil 12 and blackens and thus erases the reflex zone situated therebeneath. The erase head 12 can be set to any desired reflex zone by the triggering of input 13.

Individual reflex zones may alternatively be erased by punching out, in which case the erase head 11 is replaced by a punch head.

The erased reflex zones are also tested by means of the scanning hrad 67. In the case of 200 reflex zones, for example, 100 could be erased, i.e. 100 card tests can be carried out before the identification card requires replacement.

Referring to Figure 9, irreversible erasure of storage points or reflex zones RZ containing the forgery-proof information is carried out by means of the erase head 11, starting at the bottom line Y_1, one storage point RZ being erased during each test operation under the control of a first station 32*a* of the control stage 32 by means of information IL via input 13. The erase head 11 is on storage point X_9 in line Y_1.

On each test operation, under the control of the first station 32*a*, the scanning head 67 will scan the line containing the erased storage points and feed it as further input information to the crypto-computer. In this way, the above described fraud is impossible, since information in the old magnetic track does not agree with the new information to be erased.

In the method according to the invention, a considerable proportion of the security against forgery lies in the fact that selection of the forgery-proof information is determined by a code key applied to a crypto-computer.

This selection can readily be changed, firstly by means of the variable information IV, and secondly by changing the code key.

Security against incorrect scanning of the identification cards can be ensured by the well-known redundancy methods such as multiple storage, fault-detecting or fault-correcting codes, and so on. Faulty scanning of the optically scannable forgery-proof information due to soiling of one of the reflex zones RZ can be rendered inoperative by repeatedly scanning the card, a new reflex zone RZ being selected by the crypto-computer on each new scanning as a result of the action of the variable information.

Identification and forgery-proof storage of variable data, e.g. sums of money or time balances will now be explained with reference to Figure 9. Only one example of this will be described, but the invention is not restricted thereto.

The example relates to very high security against forgery and in many practical cases some of the steps described can be omitted.

For identification, a test operation consists of an identification phase followed by an input phase. Although the test operation starts in each case with the identification phase, the input phase will first be described.

A selection switch 30 is set to position *a* by the first station 32*a* by means of information IC. Apart from the code key information IE_1 always available, the following are fed to the crypto-computer 16:

Input information IE_3 from generator 26 for the variable information IV; and

the secret individual identification number or memorised number from a keyboard 25.

The variable information IV is recorded in the form of magnetic information IM on the magnetic track by a recording head 3*a* of the magnetic head. The information 10 from the first station 32*a* acts as information IS to control the scanning head 67 so that the latter scans the identification information ID_U as part of the forgery-proof information IU (i.e. for example, reflex zone RZ with intersection point X_1, Y_2 in zone RF of forgery-proof information) and is fed on the one hand to the first station 32*a* and on the other hand as input information IE_2 to the crypto-computer 16, in which, together with the other input information, output information IA_2 is computed and, when selection swithc 30 is in position *b*, acts as control information to re-position the scanning head 67 in pseudo-random manner. Switch 30 is set to position *c* and the partial information read off by scanning head 67 is fed on the one hadn as further identification information ID_U to the first station 32*a* and on the other hand as further input information IE_2 to the crypto-computer in which the output information IA_1 is computed and recorded in the form of magnetic information IM on the magnetic track.

In the identification phase, the selector switch 30 is again initially at *a*. The individual identification numbers are introduced into the crypto-computer 16 as input information IE_4 by means of keyboard 25. The variable information recorded during the previous test operation is read out as magnetic information IM_b from the magnetic track 2 by means of a readout head 3*b* and is fed to the crupto-computer as input information IE_3. The other operations up to generation of the output information IA_1 are the same as in the input phase. The output information IM_b magnetically stored during the previous test operation is then read out with selection switch 30 in position *c*, fed to line 46 and compared in comparator 29 with the output information IA_1 generated in the crypto-computer during the identification

phase. The result of the comparison is identity or non-identity and is available as information ID_3 at point 22. If there is identity, and if the identification information ID_U is found to be correct in the first station 32*a*, then the identification is also considered to be correct. In the first station 32*a* the identification information ID_U consisting of the forgery-proof information IU is stored for comparison for all the card-holders of the organization.

The forgery-proof storage and amendment of variable data, such as sums of money or the like, on the identification card if effected normally after the identification processes during the test operation, and also comprises two stages. During a record stage, which follows the input stage, with the selection switch 30 in position *d* for example, the instantaneous state of the account is fed in the form of digital data from a second station 32*b* of the control stage 32 in the form of an input-output unit as information ID_1 to the crypto-mixer 27 of known type, in which it is mixed with the output information IA_1 produced by the methods described above, to give the cipher, and is fed via a line 48 as magnetic information IM_a to the magnetic record head 3*a* and is recorded on the magnetic track in the form of a coded account balance.

During a read phase in the test operation following the identification phase, with selection switch 30 in position *d*, the ciphered account balance described in connection with the preceding test operation is read off from the magnetic track and fed as magnetic information IM_b via line 44 to a decode-mixer 28, in which it is decoded with the output information IA_1 produced by the method described above, and fed as the account balance in plain language to the second station 32*b*. This account balance can also be checked for authenticity by presetting a number of zeros in the second station 32*b*.

The authenticity of the account balance can also be guaranteed, for example, as described in DOS 23 50 418, by using it, firstly, as input information to the crypto-computer 16 and, secondly, storing it in "plain language" on the magnetic track. In that case, output information IA_1 generated in the crypto-computer by means of the input information:

Code key information IE_1
Forgery-proof information IE_2
Variable information IV
Account balance ID_1

is stored as a crypto-number together with the account balance ID_1 on the magnetic track 2 of the identification card during the record phase. During subsequent examination of the authenticity of the account balance during a read phase, the above-listed information is introduced into the crypto-computer and the resulting output information is checked for agreement with the stored crypto number.

For cash withdrawals from a cash dispending machine, the keyboard 25 is then used for inputting a sum of money which is dispensed by the machine and which is deducted from the account balance in the second station 32*b*, the new account balance in coded form being retained on the magnetic track in the record phase.

Falsification of the account balance stored in ciphered form is impossible because the cipher is dependent upon the code key and on the forgery-proof card information.

All the operations described are carried out digitally and electronically.

The line points 8,9,10,19,20,50 correspond to those of the simplified block schematic in Figure 2. All the other operations not described in detail in the test station are controlled by the first station 32*a* by means of the control information IST.

As already stated, the operations described apply to very high security requirements and can be greatly reduced for many applications. For example, where security requirements are less stringent, the forgery-proof information can be omitted or just one card number may be provided and the card information may be contained in the magnetic track. If requirements are somewhat higher than this, just a single track, e.g. line Y_1 in Figure 2 of forgery-proof information could be provided, for example, and be simultaneously scannable with the magnetic track during the period when the card passes through the test station. The forgery-proof information selected by the crypto-computer, by means of code key and variable information, could also serve as crypto-computer input information in order jointly to determine the output information IA.

To eliminate errors during card scanning, the forgery-proof information may be stored in redundant error-correcting codes of known type. For example, each storage point RZ could be tripled, being distributed over the card, and the two identical readings of the three being selected as the correct ones.

Using the variable information, it would also be possible to carry out additional test operations if one such operation is unsuccessful, e.g., due to card soiling, a changeover to perfectly readable storage points being made by the pseudo-random selection of the forgery-proof information.

All control operations and ciphering can be carried out by means of one or more micro-processors, all the operations being in sequence as a result of the relatively slow

processes and the outlay required for control of the test operations for higher security will also be relatively small.

WHAT WE CLAIM IS:–

1. A process for coding and subsequently testing an identification card having a first area in which machine readable information is stored in permanent form and a second area in which machine readable information may be recorded and erased, the coding process comprising providing secret information, ciphering at least some of the permanently recorded information with said secret information to provide identification informtion and recording said identification information in said second area; the testing process comprising providing secret information identical to that provided on coding the card, selecting and machine reading from the card those areas containing the permanently recorded information used for ciphering to provide identification information, machine reading the identification information recorded in said second area and comparing it with the identification information formed during the testing process.

2. A process according to Claim 1, including using another set of extra information with at least some of the permanently recorded information and the secret information to form said identification information recorded in said second area, recording said another set of information in said second area and, on testing the card, machine reading said another set of information to form the identification information used in said comparison.

3. A process according to Claim 2, including forming selection information from cyphering the secret information with at least some of said another set of information and selecting said first areas under control of said selection information.

4. A process according to Claim 1, including cyphering data information by the identification information and recording the ciphered data on the card and recovering the data information during testing by deciphering with the identification information read from the card.

5. A process according to Claim 1, including irreversibly erasing some of the permanent information from the card and utilising an erase information obtained from the erased state of the permanent information to form the identification information and the test information.

6. A process according to Claim 2, including using a different serial number as the extra information on each test operation.

7. A process according to Claim 2, including using date-time as the extra information.

8. A process according to Claim 2, including using random information as the extra information.

9. A pricess accordine to Claim 1, including using a predetermined part of the permanent information as recognition information containing the identity of the cardholder.

10. A process according to any one of the preceding claims, characterised in that certain parts of the permanent information determined by the identification information are used as recognition information.

11. A process according to Claim 1, wherein the permanent information on the identification card is represented by a spatial arrangement of a plurality of optical reflex surfaces which are embedded in the card and which are not accessible to mechanical scanning, and all the other information is stored on a magnetic track.

12. A process according to Claim 11, wherein groups of reflex surfaces are combined into reflex zones and at least one of these zones is selected by the selection information for ciphering.

13. Identification apparatus using identification cards bearing two sets of machine-readable information, one set being stored in permanent form and the other in variable form, and comprising a production and test station for the identity card, said station comprising first means for reading the permanent information, second means for reading the variable information and first recording means for variable storage of information on the identification cards, and an evaluation stage cooperating with the two reading means and the first recording means wherein the evaluation means a.nd the first recording means wherein the evaluation stage contains a store for a secret key information, a decision stage and a crypto-generator which generates a first output information from the secret key information stored in the store and the permanent information read off from each card by the first reading means, the decision stage during card testing tests the first output information as test information to see whether it agrees with the variable information read off as identification information from the card by the second reading means and when a card is made out the recording means store the first output information in the form of identification information on the card.

14. Apparatus according to Claim 13, wherein the evaluation stage comprises a generator which is connected to the crypto-generator and which is intended to produce extra information which varies from one test to another, said apparatus including second recording means for storing this extra information on the identification cards and third reading means which read the extra information from the identification cards, and

wherein the crypto-generator generates the first output information from the key information, the permanent information read off by the first reading means, and the extra information read off by the third reading means.

15. Apparatus according to Claim 14, wherein the second and first recording means and the second and third reading means are identical.

16. Apparatus according to Claim 13, including means connected to the crypto-generator to feed memory information to the crypto-generator, and the latter takes this memory information into account when generating the first output information.

17. Apparatus according to Claim 14, including means for selecting parts of the permanent information stored on the cards, and wherein the crypto-generator generates a second output information from the secret key information and from the extra information read off by the third reading means, and on the basis of this second output information the selection means select the parts of the permanent information.

18. Apparatus according to Claim 14, wherein the card making and test station comprises an input and output stage for data information, a crypto-mixer and the crypto-generator, said mixer ciphering the data information by means of the first output information, third record means for storing the ciphered data information on the identification cards, fourth reading means for reading the ciphered data information stored on the identification cards, and a decipher-mixer which is triggered by the fourth reading means and the crypto-generator and which is connected to the input and output stage and which, by means of the first output information, deciphers the ciphered data information read off by the fourth reading means and passes it to the output and input stage.

19. Apparatus according to Claim 18, wherein the second and the fourth reading means and the first and third recording means are identical.

20. Apparatus according to Claim 19 or 20, wherein the input and output stage is a cash dispensing machine with an account balance device, and has input means by means of which it is possible to input the value of a sum of money to be drawn from a credit account defined by the identification card, the account balance device feeds to the crypto-mixer in the form of data information the account balance revised after the withdrawal, and before any payment is made said device compares the old account balance read off from the identification cards and deciphered by the decipher-mixer with the amount of the input sum of money to be withdrawn, and prevents any payment from being made if such sum is greater than the account balance.

21. Apparatus according to Claim 13, wherein the card making and testing station has a selection stage which selects parts of the permanent information as identification information.

22. Apparatus according to Claim 13, wherein the card making and testing station has an erase head and positioning means for the erase head, such means irreversibly erasing parts of the permanently stored card information which are selected on each test on an identification card.

23. A process according to any one of Claims 1 – 3, wherein memorized information is additionally used to form the identification information.

TREGEAR, THIEMANN & BLEACH,
Chartered Patent Agents,
Enterprise House,
Isambard Brunel Road,
Portsmouth PO1 2AN
–and–
49/51, Bedford Row,
London, WC1V 6RU
Agents for the Applicants

Printed for Her Majesty's Stationery Office, by Croydon Printing Company Limited, Croydon, Surrey, 1979.
Published by The Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.

Fig.1a

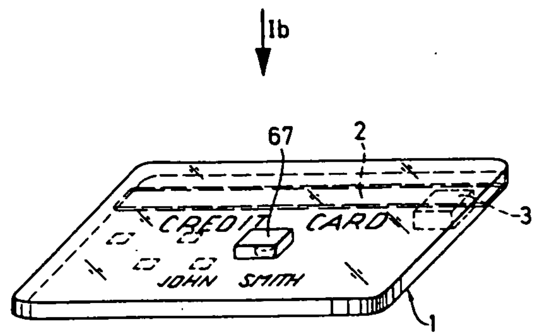
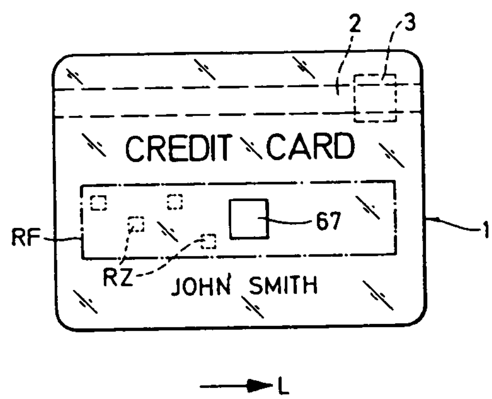

Ib
67
2
CREDIT CARD
3
JOHN SMITH
1

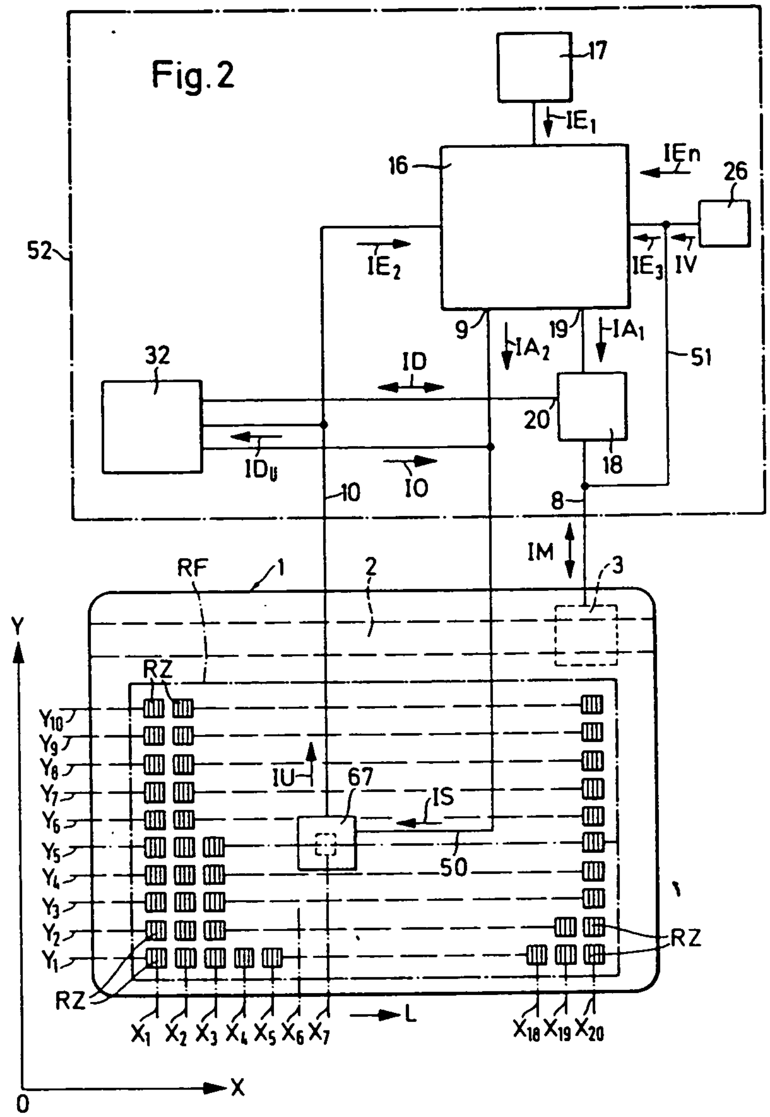
Fig.1b


2
3
CREDIT CARD
67
RF
1
RZ
JOHN SMITH
L

1546053 COMPLETE SPECIFICATION

7 SHEETS *This drawing is a reproduction of the Original on a reduced scale*

Sheet 2



1546053 COMPLETE SPECIFICATION

7 SHEETS *This drawing is a reproduction of the Original on a reduced scale*

Sheet 3

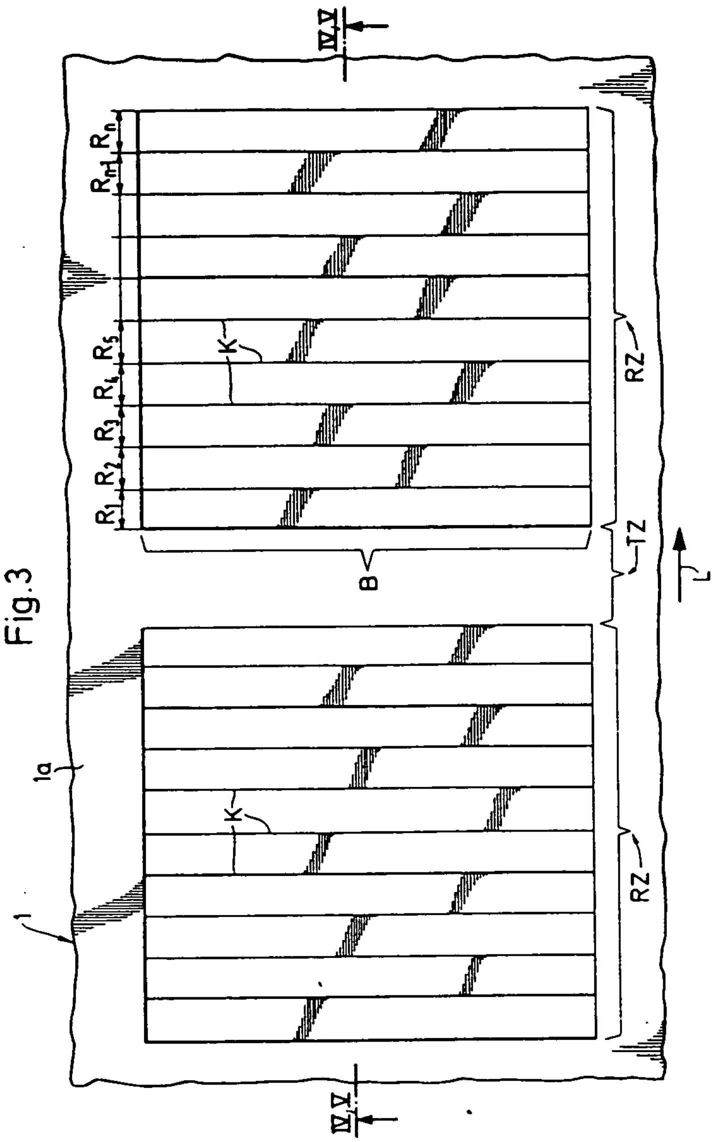


Fig.3

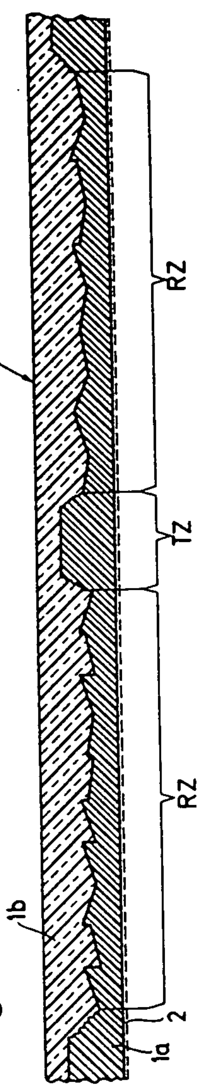


Fig.4

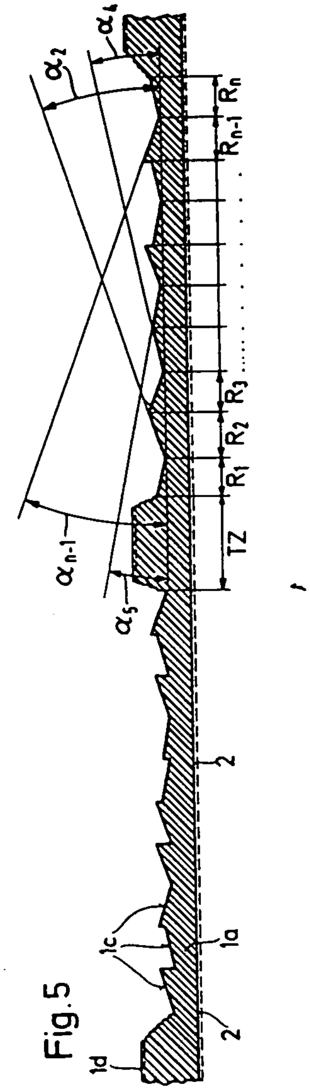
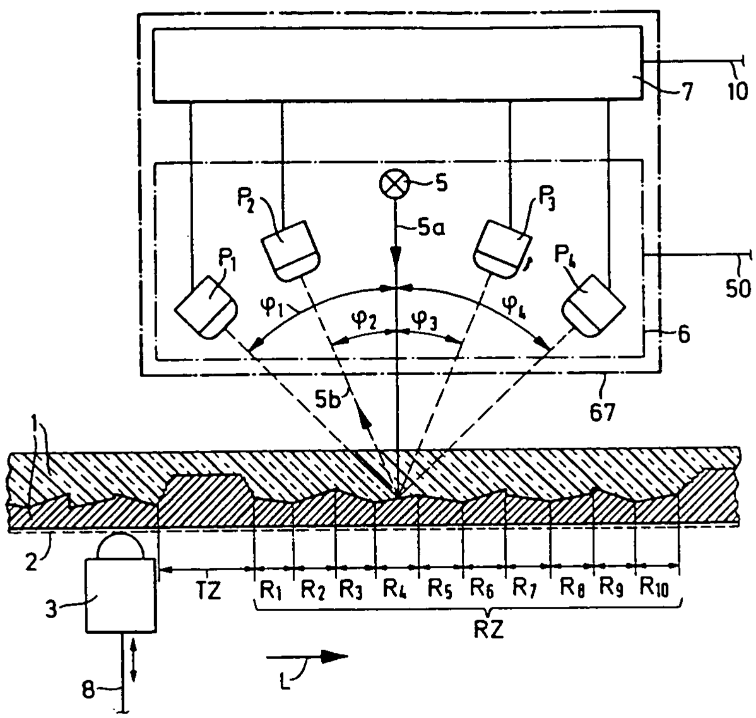


Fig.5

Fig.6


7
10
5
5a
P1
P2
P3
P4
φ1
φ2
φ3
φ4
50
6
67
5b
1
2
3
8
TZ
R1
R2
R3
R4
R5
R6
R7
R8
R9
R10
RZ
L

1546053 COMPLETE SPECIFICATION

7 SHEETS *This drawing is a reproduction of the Original on a reduced scale*

Sheet 6

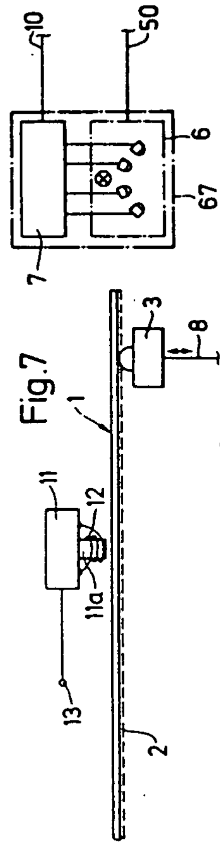


Fig.7

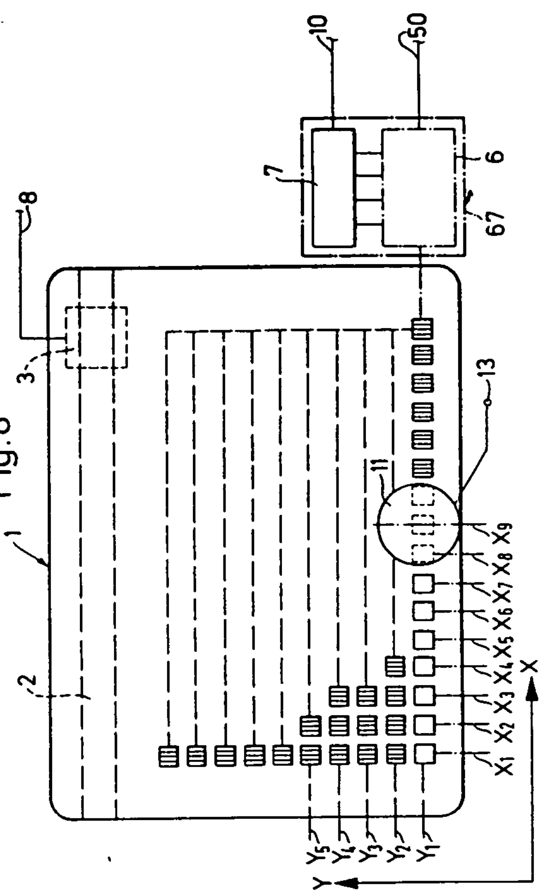
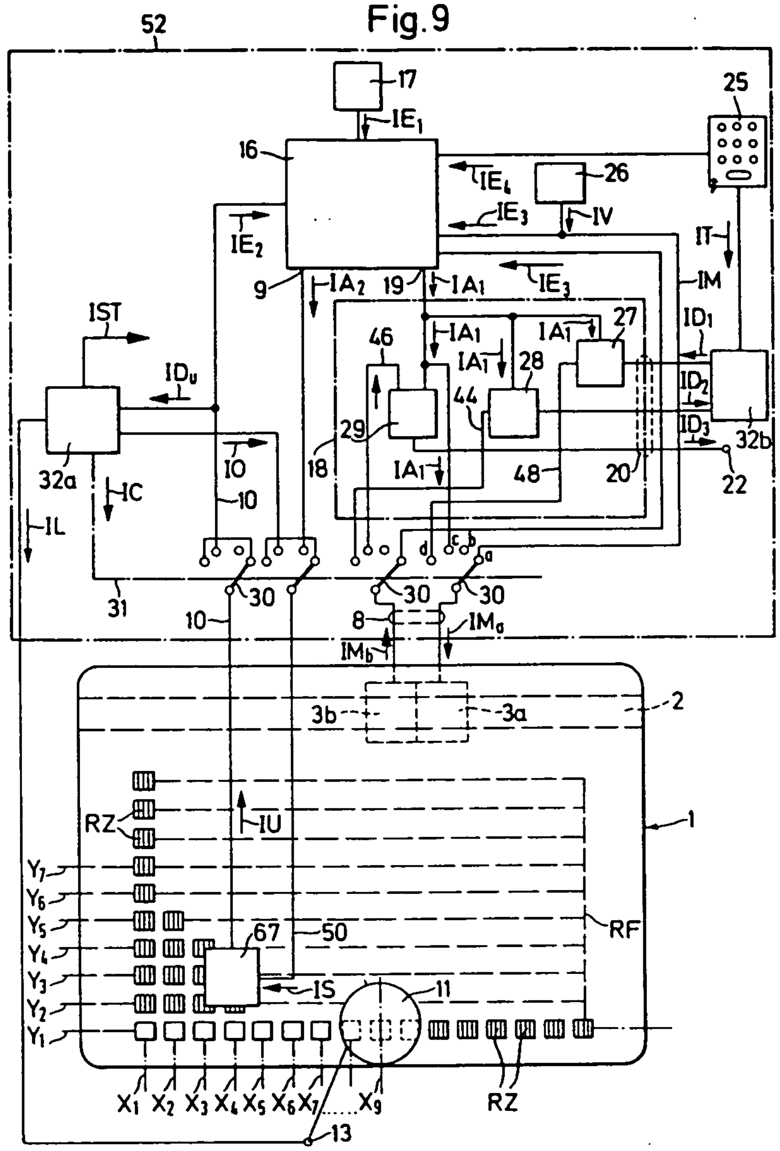


Fig.8

Fig.9


52
17
IE1
16
IE4
26
IE3
IV
25
IT
IM
IE2
9
IA2
19
IA1
IE3
27
ID1
IST
46
IA1
IA1
28
ID2
IDu
29
44
ID3
32b
IO
18
IA1
48
20
22
32a
IC
10
IL
31
30
10
8
IMa
IMb
3b
3a
2
RZ
IU
1
Y7
Y6
Y5
67
50
RF
Y4
Y3
IS
11
Y2
Y1
X1 X2 X3 X4 X5 X6 X7 X9
RZ
13